RSAC 2025 Conference

Many Voices.
One Community.

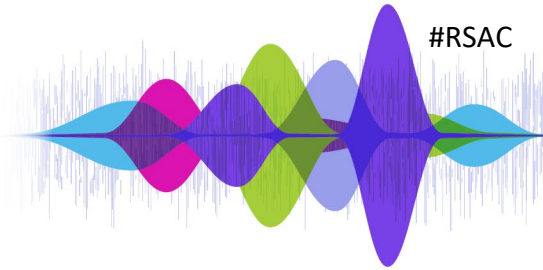
SESSION ID: PART2-W01

2025 and Beyond: The Evolution of Identity-Centric Cybersecurity

Vivin Sathyan

Chief Technology Consultant
ManageEngine (part of Zoho Corp Pvt. Ltd)

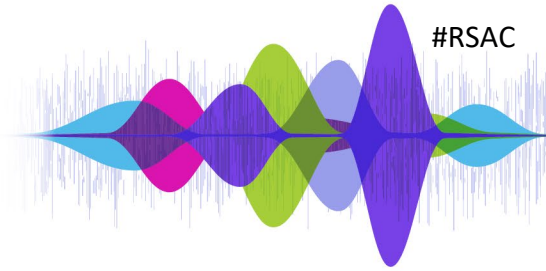
Disclaimer



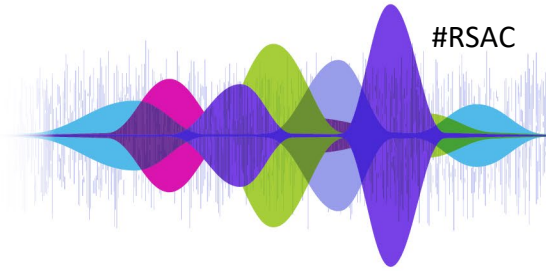
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.



Know about Melatonin?



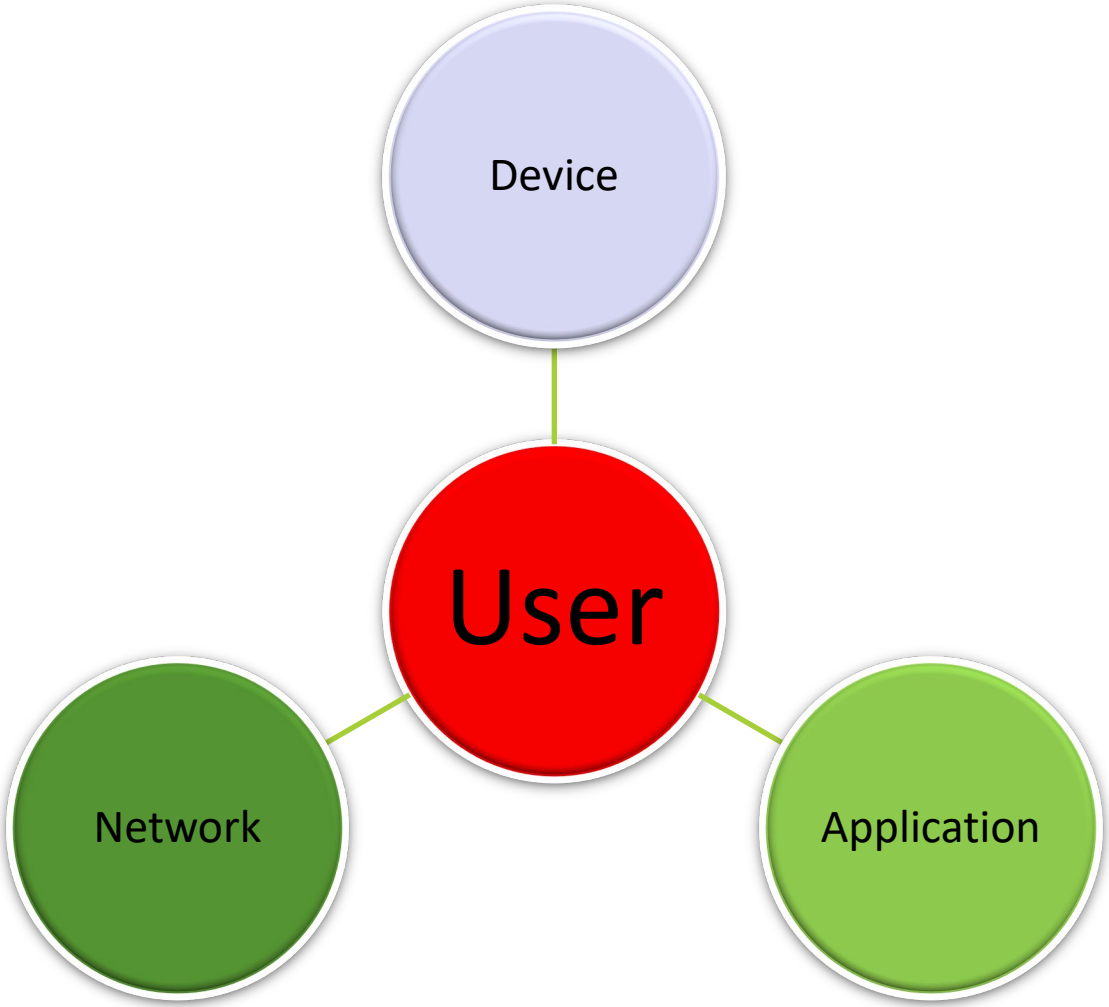
Melatonin is a natural hormone that's mainly produced by your pineal gland, which is a tiny gland in your brain. Your brain releases it when you **sleep in complete darkness.**

I have been doing tech talks for 13 years and…

I HAVE OBSERVED THAT MELATONIN ALSO GETS SECRETED DURING A TECHNICAL SESSION…..

Let us fight melatonin for the next 45 minutes!

Common Identities in a Digital Infrastructure

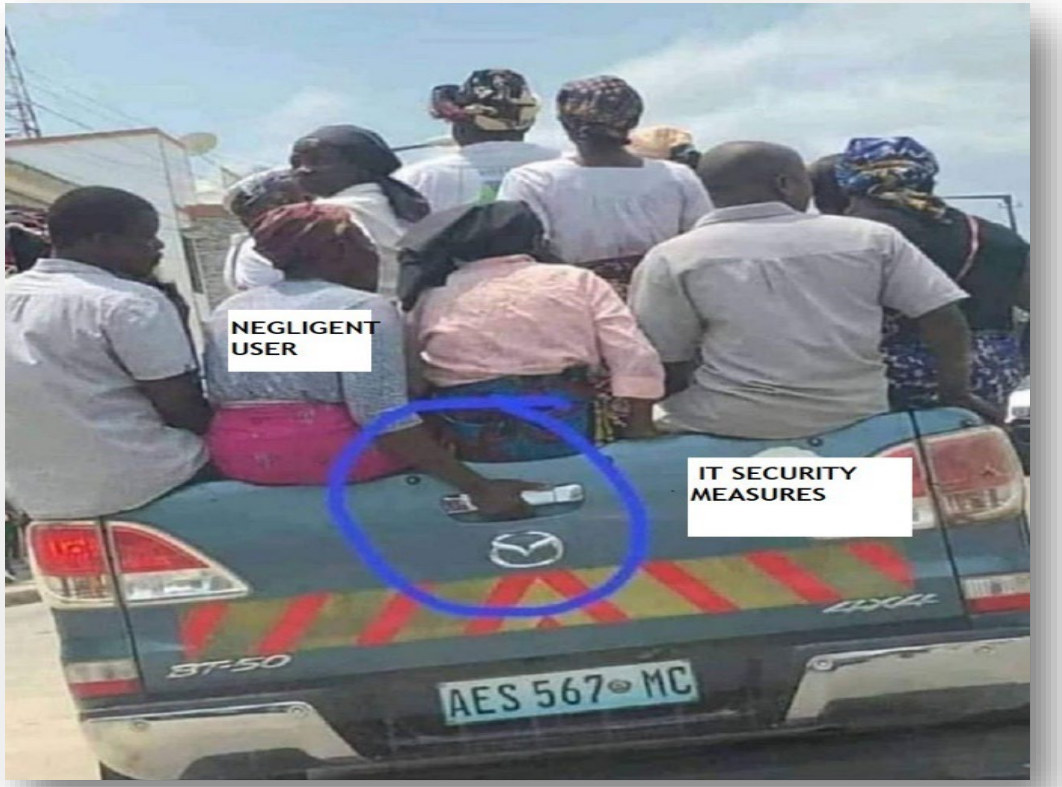


I am not worried about this

#RSAC
RSAC 2025 Conference

I am worried about this – Admin error!

I am worried about this – User error!



User education is good but it has to be contextual

RSAC 2025 Conference

Objective: Securing User Identities

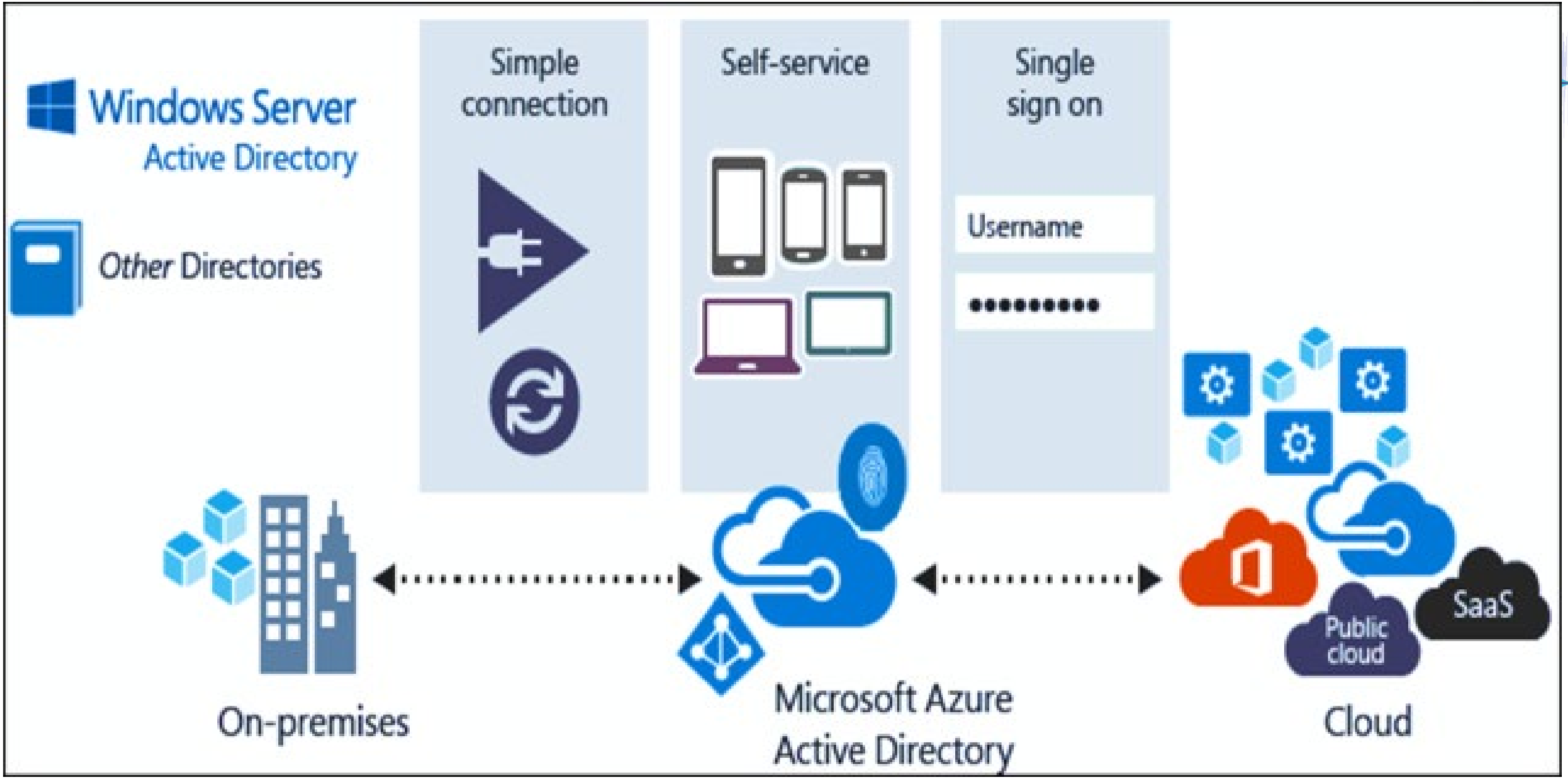
Where do we begin the whole process from?

Let us start with Active Directory

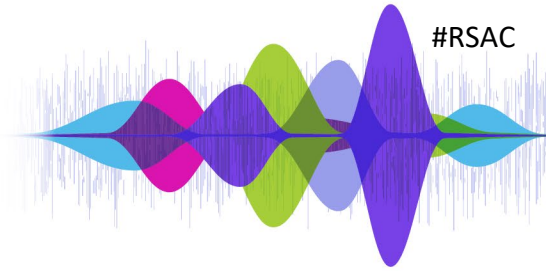
Live (if the internet works) Active Directory Hack

3-stage attack

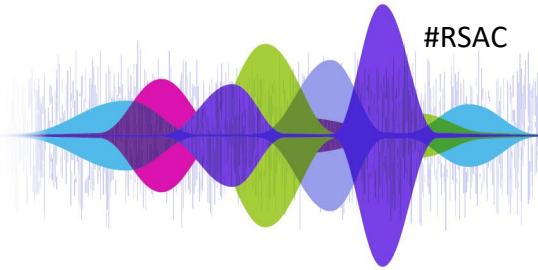
1. Copy ntds.dit and system file.
2. Extract password hashes from ntds.dit using system file.
3. Crack hashes to reveal user passwords.



RSAC 2025 Conference



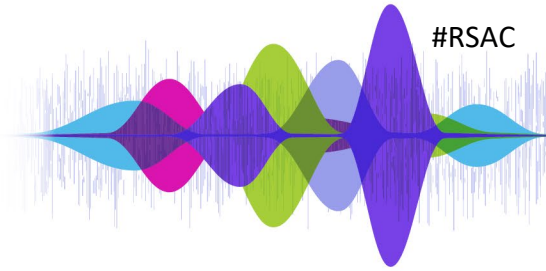
Before talking about securing user Identities let us understand the new network perimeter.



The new network perimeter

- In on-premises IT infrastructure and traditional security models
  - Easier verification and authorization of everything inside the corporate network, including devices, users, applications, and servers.
  - External users are validated via VPN and NAC.
- With the increasing adoption of the cloud and remote work
  - Data is stored outside of corporate walls
  - Users access enterprise applications that are located on the cloud/on-premises using various types of devices from locations outside the corporate network

The result – Soft boundaries!



Hybrid AD is a crucial component of the new network perimeter

Best of both worlds – Hybrid AD

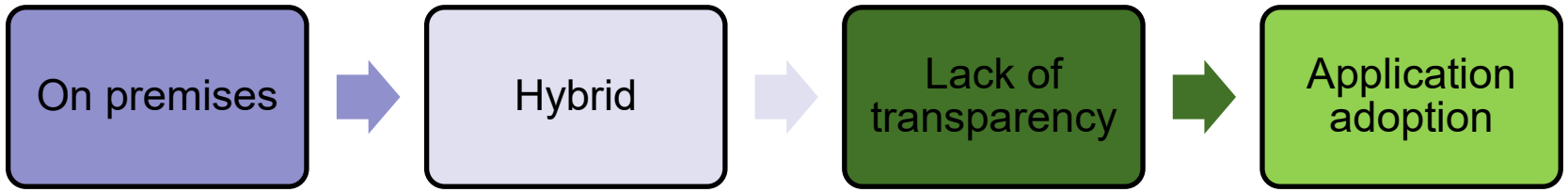
As companies embark on application and data modernization, they should consider using a hybrid AD, as it balances the application and data workload across both platforms.

Innovation, speed, storage, and scalability of the cloud
Regulatory compliance, performance, and data gravity of on-premises
Hybrid AD

Problem with the cloud – lack of visibility

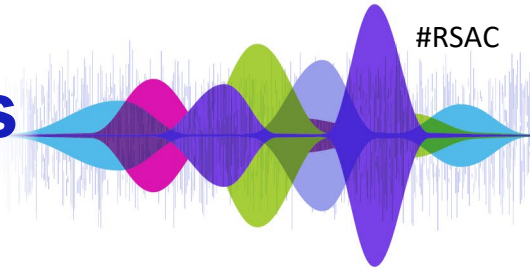
Closing the security gap in the cloud

- In on-premises infrastructures
  - Managing identities, authentication, and access is relatively easy with Microsoft's Lightweight Directory Access Protocol (LDAP) and Active Directory (AD).
- In the cloud
  - It is much more difficult for IT departments to monitor which users are accessing which applications and services.
  - Solution: Adopt more applications ☺

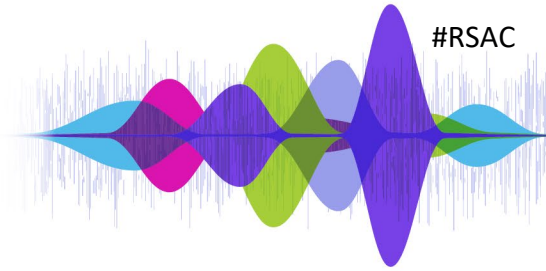


A new challenge!

THE new challenge – managing fragmented identities



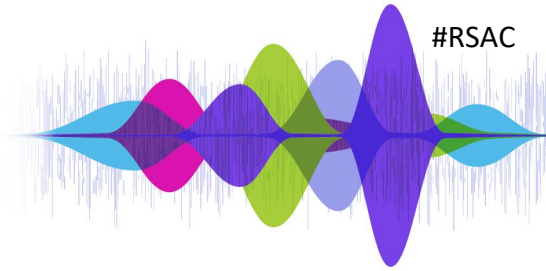
- Ensuring secure access to every user, application, and device, irrespective of their location.
- The access should be contextual
- IT administrators have to create access policies based on location, IP address, device etc.



Problem: Managing and Securing fragmented user Identities.

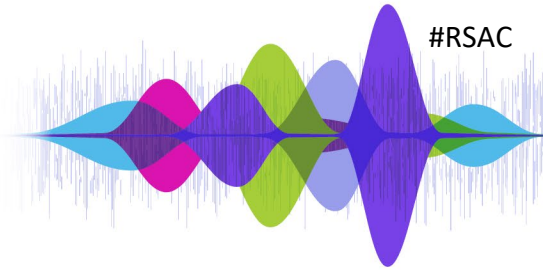
Solution?

Implement Zero Trust



But…

Implement Zero Trust – From a concept to reality

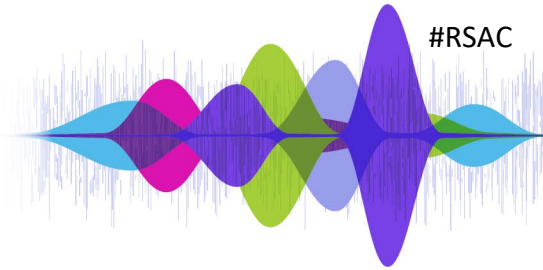


- How many of you have successfully implemented Zero Trust?

John Kindervag would be sad!

Creator of the Zero Trust Security Model - 2010

Practical Steps to Secure user Identities

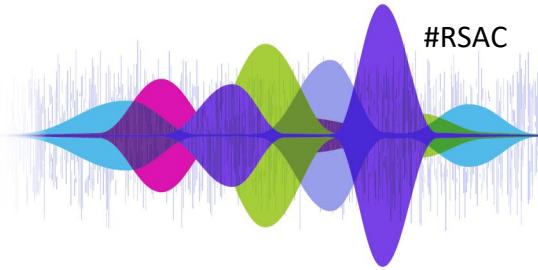


- Performing Identity risk assessments to proactively mitigate security breaches.
- Using access certification campaigns to attest or revoke privileges periodically.
- Integrating HCM applications and employee databases for automated onboarding, off boarding, and clean up.
- Implementing Roll based access control (RBAC)
- Strengthening two layers of authentication – Passwords and Contextual MFA

RSAC 2025 Conference

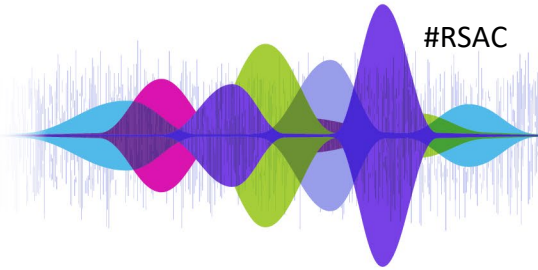
Active Directory Risk Assessment

Common threats to AD security



- Default Security Settings
- Inappropriate Administrative Users and Privileged Access
- Inappropriate or Broad Access for Roles and Employees
- Vulnerable Passwords for Administrative Accounts
- Unpatched Vulnerabilities on AD Servers
- Lack of Visibility and Reporting of Unauthorized Access Attempts

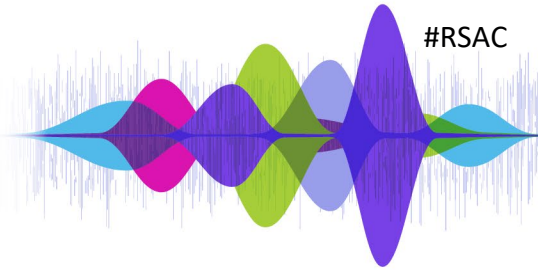
Active Directory Risk Assessment



- Provides **critical insight** into the health of your directory service (performance, configuration, and event data)
- Expose the risks by applying **various rules/filters** on AD data and also provide plan to remediate them.

E.g., Admin users with "Password Never Expires", User accounts with "Reset password" permission, Files and folders accessible by "Everyone" and etc.

Active Directory Risk Assessment

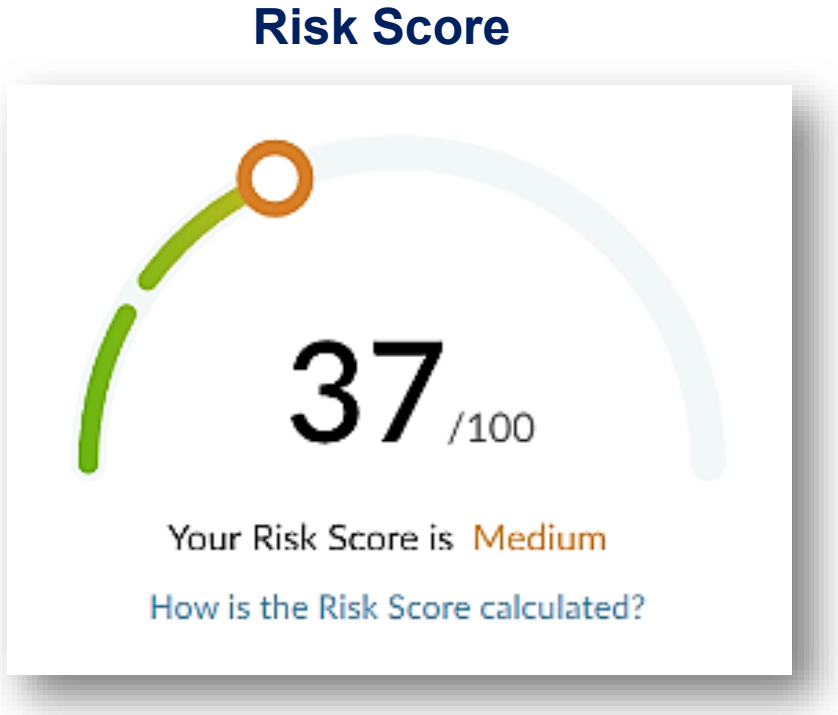


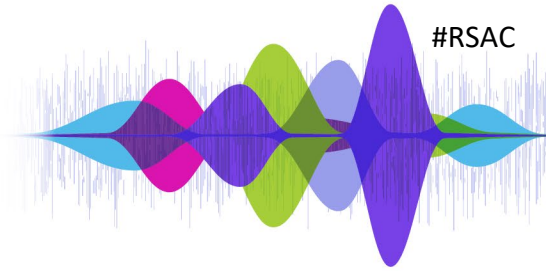
- Involves identifying and assessing the risks that could affect the IT Assets
- It also helps to finding the likelihood, Impact and Severity of the identified risks using a Risk Model (***NIST***, ***OWASP***, and ***DREAD***)
- **Risk = Likelihood * Impact**

For example, "Administrative Inactive Users" is a high risk indicator, if any one user is compromised it could affect the entire AD environment.

Active Directory Risk Assessment

- Can generate risk assessment once you configure a domain
- Daily automated risk assessments at 4 am.
- Presentation of 39 risk indicators, each assigned with a specific weightage based on its severity and impact.
- Risk exposure calculated as: (Number of Risky Users / Total Users)
- Capability to export comprehensive Risk Assessment details, encompassing all 39 risk indicators and associated risky user details.





Risk Categorization

Critical, High, Medium, and Low.

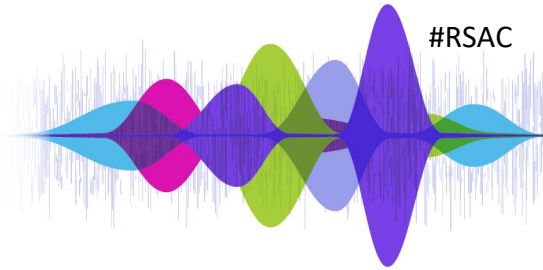
Risk Mitigation

Map security frameworks (MITRE, ANSSI), associated with a specific risk indicator, and remediation measures.

RSAC 2025 Conference

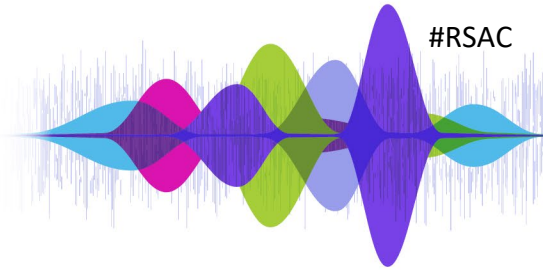
Access Certification & Entitlements

Access Certification Campaign (ACC)



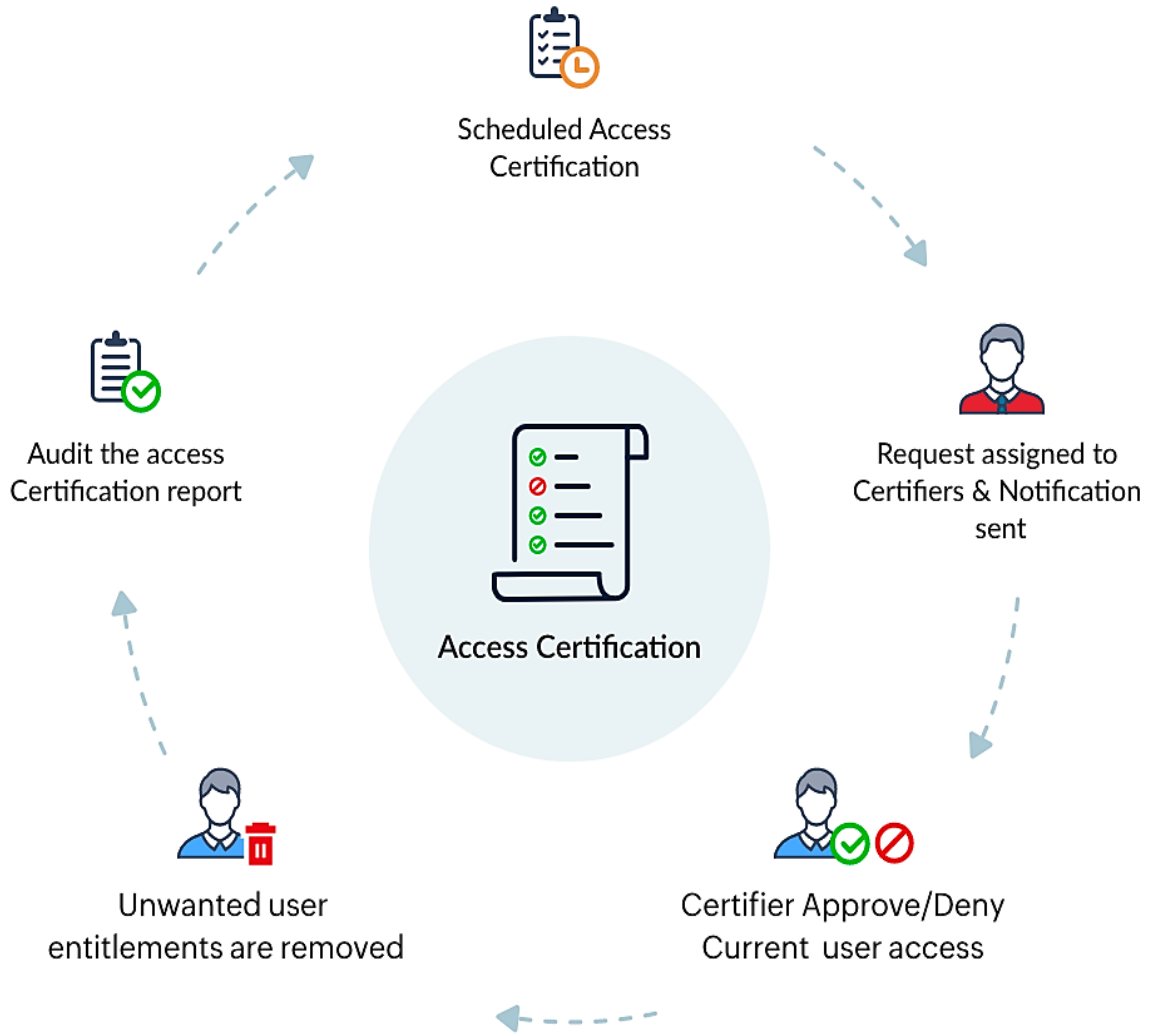
- One of the prominent IGA feature
- Process of reviewing and validating the access rights and privileges granted to Users/Groups periodically
- Ensure that only authorized individuals have access to sensitive data, systems, and resources.
- Based on Principle:
  - Zero-Trust Model : Never trust, always verify
  - Ensuring right people have right access.

Importance of Access Certification



- As employees move team or leave company, simplify the process of **revoking** their old privilege.
- Enhances **accountability** within your organization by assigning responsibility to individuals for their access rights.
- Plays Crucial role to identify who needs **permanent privileged access** permissions.
- Detecting potential **insider threats** by identifying unauthorized access and privilege misuse within internal network.

Access Certification Flow Chart


Scheduled Access Certification
Request assigned to Certifiers & Notification sent
Certifier Approve/Deny Current user access
Unwanted user entitlements are removed
Audit the access Certification report
Access Certification

RSAC 2025 Conference

Onboarding by avoiding permission bloat

Ability to manage multiple platforms

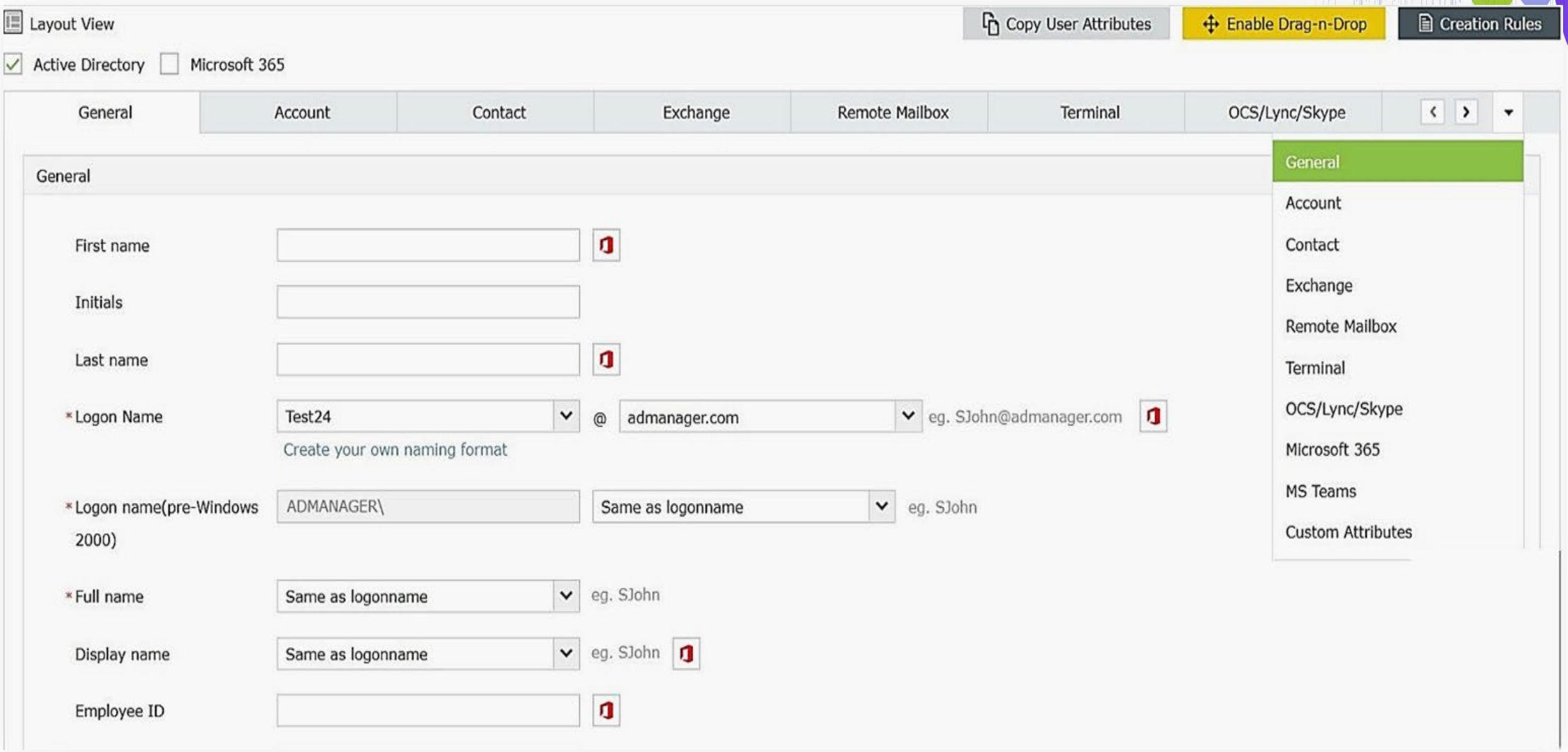
Microsoft 365

Google Workspace

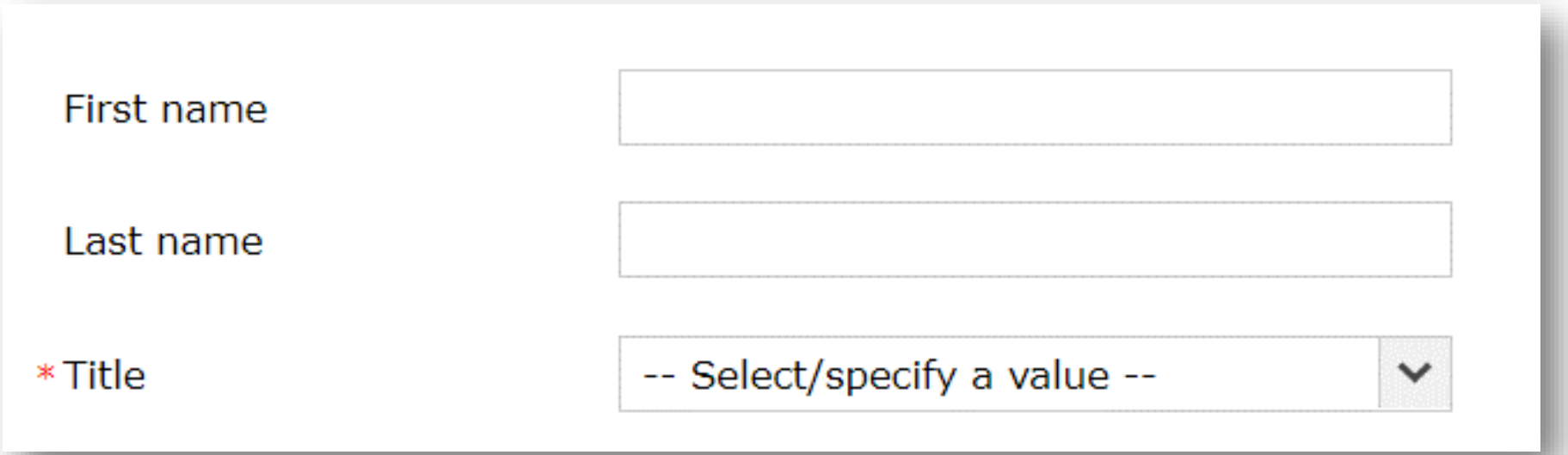
Microsoft Active Directory

Microsoft® Exchange Server

Maintain standardization for all accounts



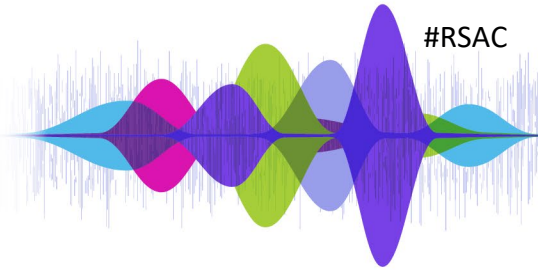
Layout for the Technician – User creation



RSAC 2025 Conference

Delegation - RBAC

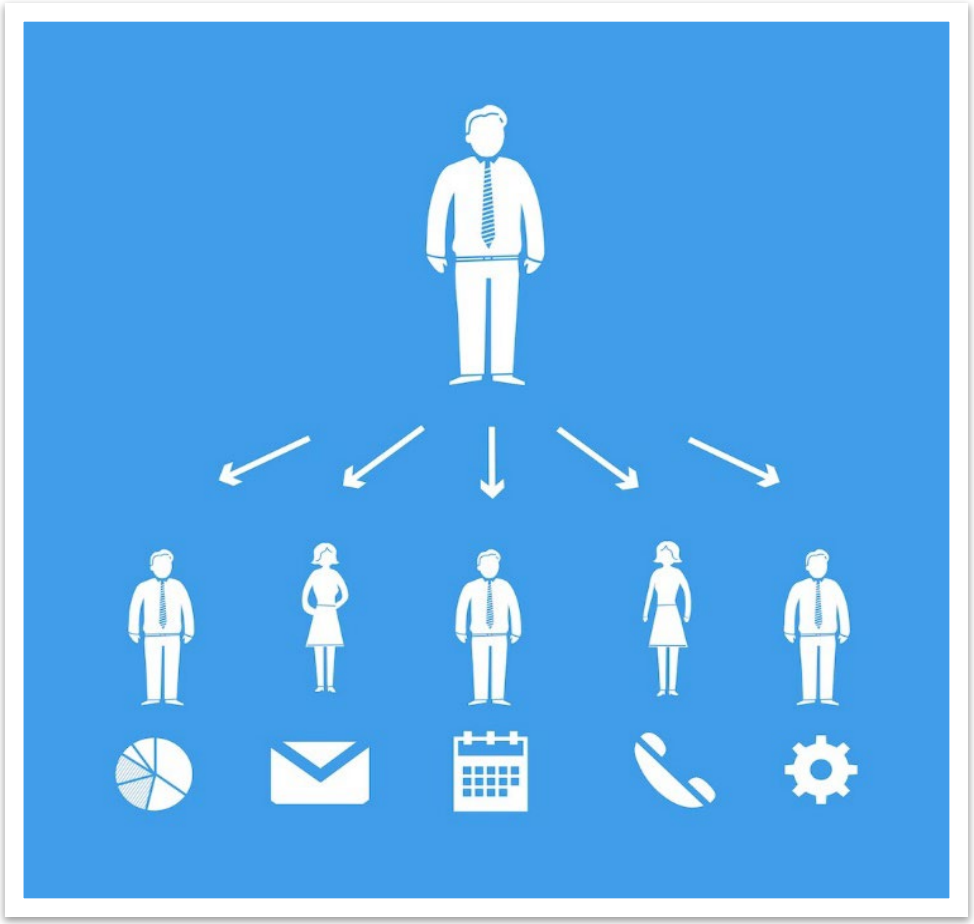
Delegation has to be non-intrusive



Points to be remembered

- Precise restrictions (actions, users, groups, OUs, even attributes!)
- Use the domain admin account only for actions that require the privilege level of this account.
- Never use shared accounts
- Review events and take corrective actions

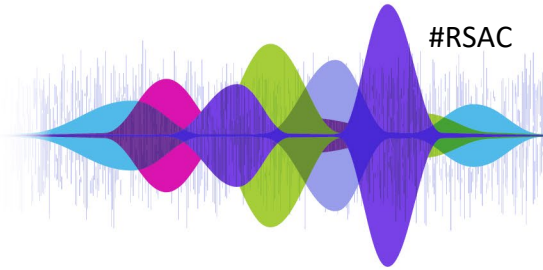
Delegation has to be non-intrusive



RSAC™ 2025 Conference

Automation

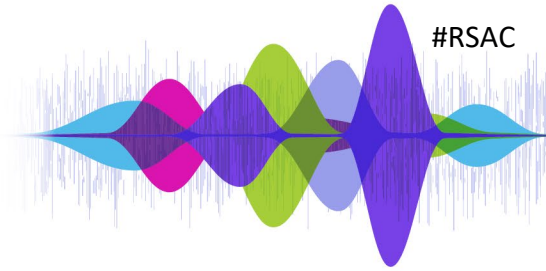
Automate routine AD tasks for efficiency



- **AD account provisioning/de-provisioning (includes AD clean up)**
- **Clean up includes,**
  1. **Users** who have not logged in for more than 180 days and are still enabled
  2. **Computers** that have not authenticated for more than 6 months
  3. **Groups** without any members
  4. Unused **GPOs**

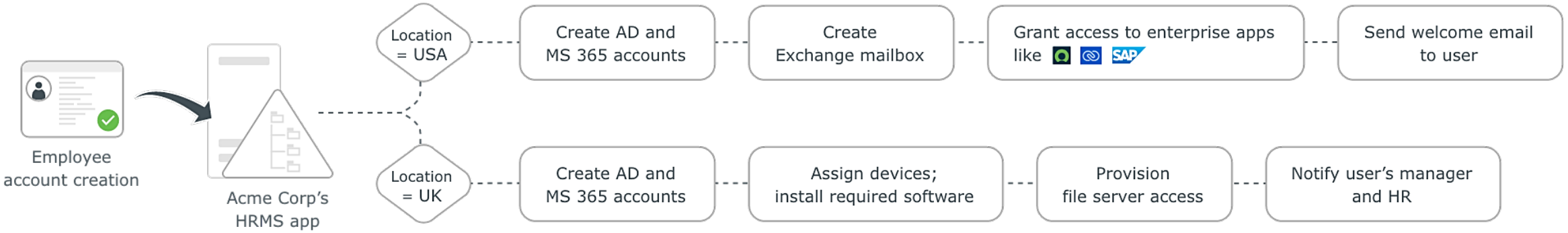
Automation - Expectation

Automation – Reality (at times)

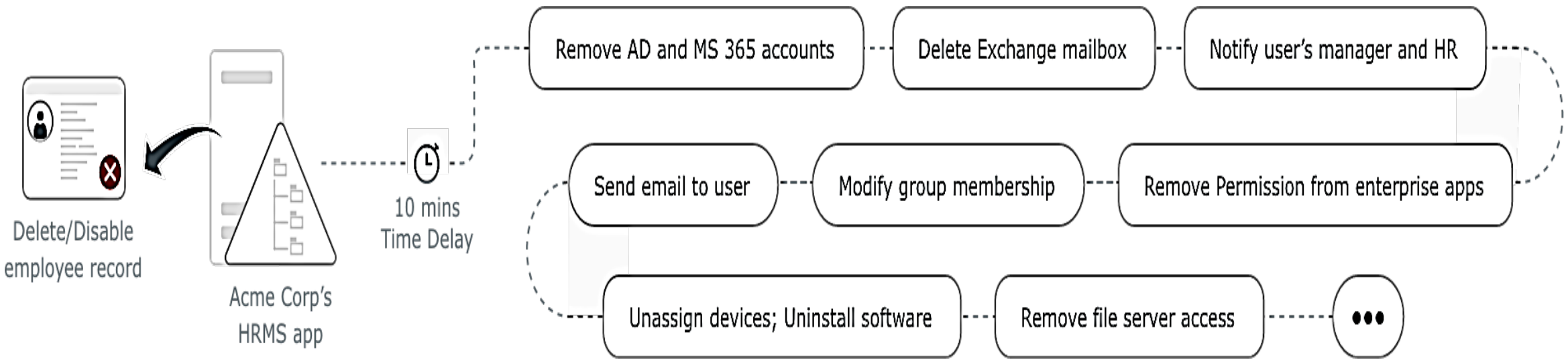


Supervise and execute critical automations, please!

Orchestration – User onboarding



Orchestration – User offboarding

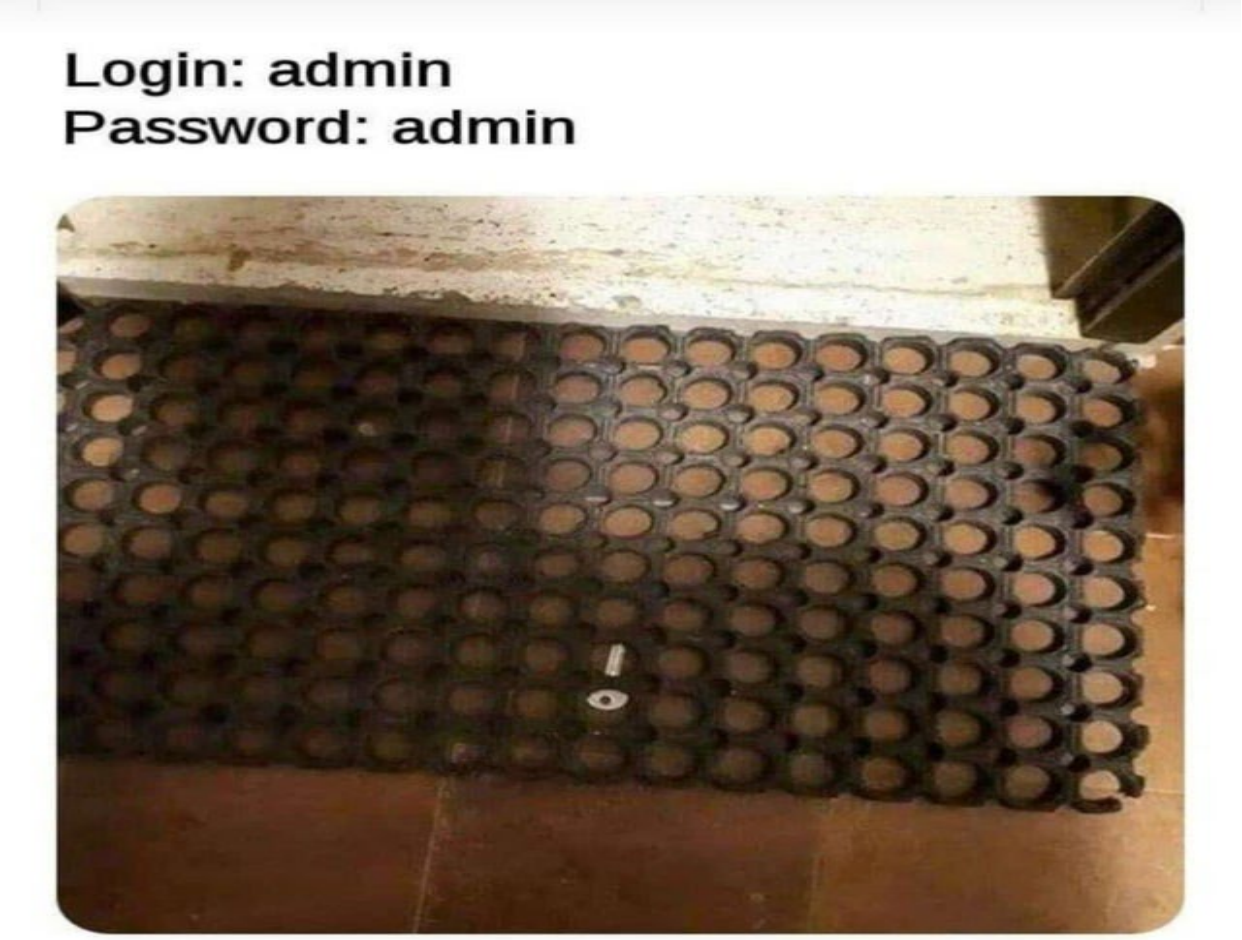


RSAC™ 2025 Conference

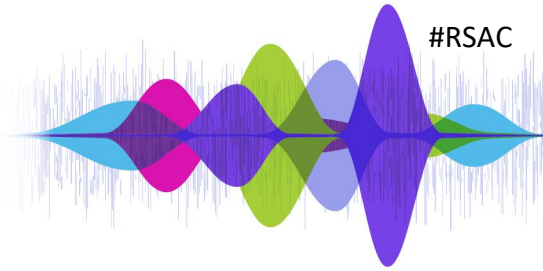
Authentication

Humans are the weakest link in IT Security!

Old habits seldom die!

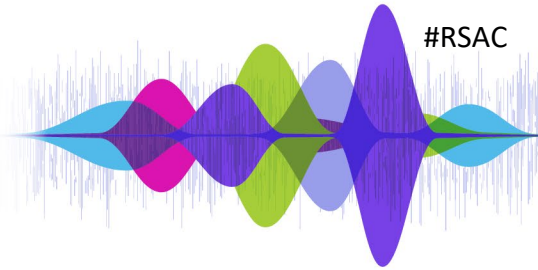


Authentication checklist



- ✓ Secure remote logon attempts
  - Secure both local and remote login attempts to servers and workstations.
- ✓ Defend against credential-based attacks
  - Mitigate all credential-based cyberattacks, including brute force, password spray, and dictionary attacks.
- ✓ Ensure regulatory compliance
  - Meet NIST SP 800-63B, NYCRR, FFIEC, GDPR, and HIPAA compliance mandates.

2 layers of authentication - one policy



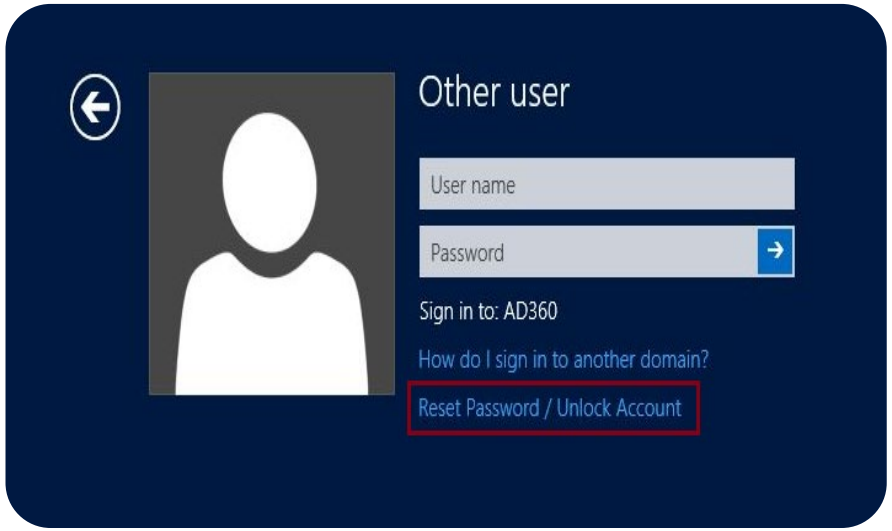
Layer 1 – Strengthening passwords

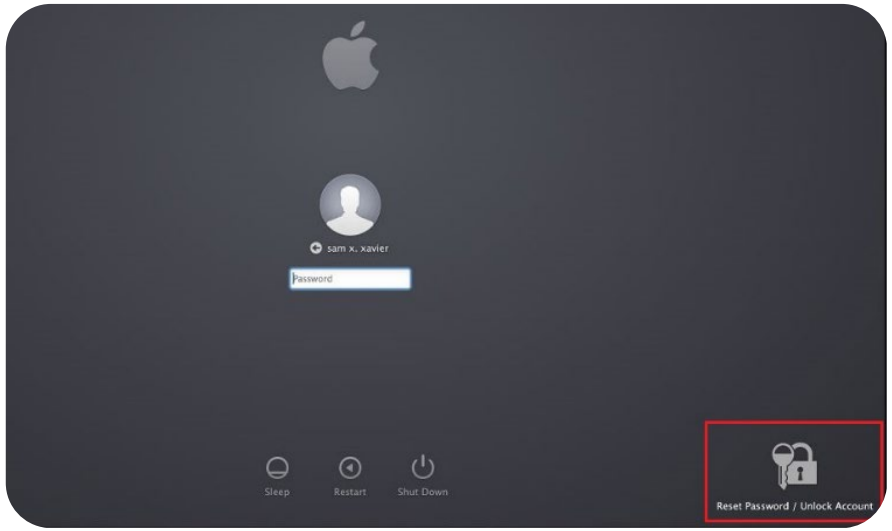
- Without disturbing your existing password policy
- Enabling password self-service

Layer 2 – Contextual MFA

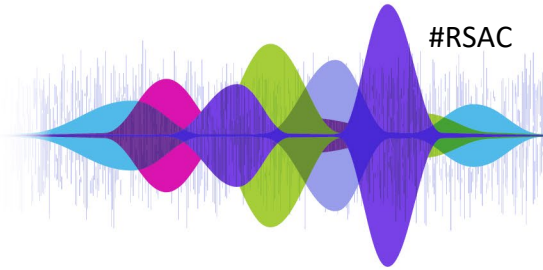
- MFA for endpoints
- MFA for applications
- MFA for VPN
- MFA for Password change/Reset

Secured self-service is the way forward!





MFA must-have points



- **In the next 30 days you can do this for all your users in the org**
- **Endpoint multi-factor authentication (MFA):** Linux/Windows/MacOS logins and cloud applications.
- **Integration with 'Have I Been Pwned?',** which prevents the use of breached passwords during password change or reset by users.
- **MFA for VPN:** Secure your VPN by enabling MFA via fingerprint/Face ID, Push Notification, Google Authenticator, Yubico OTP, and other wide range of authentication factors.

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank you

Vivin Sathyan